TRUSTED COMPUTING GROUP (TCG) TIMELINE
October 2012

2003

Trusted Computing Group is announced with membership of 14 companies, including Promoters and board members AMD, Hewlett-Packard, IBM, Intel Corporation, Microsoft, Sony Corporation, and Sun Microsystems, Inc. TCG structure and vision are created to enable extension of trusted computing beyond the PC into the enterprise. TCG adopts existing specifications for the Trusted Platform Module (TPM) security chip for clients and publishes as an open industry specification.

2004

TCG announces the Trusted Platform Module (TPM) specification 1.2. Manufacturers begin shipping a variety of enterprise desktop and notebook PCs equipped with TPMs and software to enable applications including data and file encryption, secure email, single sign-on, storage of certificates and passwords, and other applications.

Members begin participating in work groups to address security in mobile devices, storage, servers, peripherals, and infrastructure requirements.

TCG also announces the Trusted Network Connect (TNC) subgroup to work on an open specification for network access control and endpoint integrity and the addition of almost 30 new members to focus on the effort. Group starts to define requirements and use cases for an open specification.

Membership expands to 98 companies by end of the year, with participation broadening beyond semiconductor and client companies to software developers, networking, and storage companies. The group initiates an advisory council of leading IT, privacy, finance and security industry experts.

The group also begins a liaison program with other industry standards groups and begins a mentoring program for those researchers and academic institutions doing research on trusted computing and related topics.

2005

The group expands its board of directors. Two companies, VeriSign and Seagate Technology, are elected by the membership to the board. Infineon, an early developer and adopter of the TPM, is added to the board as a Promoter member.

TPM adoption continues to grow as chipmakers offer discrete and integrated versions for desktop and notebook systems, as well as for servers. Analysts predict shipments to top some 250 million by 2010.

The group's Mobile Phone Work Group releases use cases to define how the concepts of trusted computing could be applied in mobile phones. Work group participation expands to include key vendors in handsets, chips, and applications.

Hoping to offset the rapid increase in data loss, theft, and unauthorized access, the Storage Work Group begins work on an open industry specification for data "at rest" in a variety of mediums, including hard drives, tape, and flash memory. The group releases its use cases for industry review and begins working with existing storage specification groups to ensure command support is created for widely used SCSI and ATA architectures.

The Server Work Group makes its specification for using the TPM in servers available. Vendors begin development of servers that will help ensure a trusted client is connecting to the intended server. The specification also provides for a usage model in which the server is verified to meet minimum standards before being allowed to perform sensitive transactions.

TNC participation swells to some 60 member participants. TCG delivers the TNC architecture and a series of open specifications for developing products to support it. Several demos are shown to demonstrate some key concepts of TNC at Interop Las Vegas. First products, including switches and other products, are announced as supporting TNC. Microsoft pledges interoperability of its Network Access Protection architecture with TNC.

2006
Shipments of TPMs for systems are predicted to top some 20 million and virtually every enterprise system shipped from the top 20 vendors contains one of the security chips. The first servers enabled with TPMs begin shipping.

Infineon and Lenovo join TCG's board of directors as Promoter companies. Wave Systems and Seagate Technology are elected to the board by the membership of some 140 member companies.

TNC adds specifications to the architecture. A more robust demonstration incorporating integrity measurement and verification and other key TNC functions is shown. The first deployment, a telemedicine application, is announced. The Internet Protocol Equipment Certification organization of Japan endorses TNC for network security. Ten more industry companies, including those in remediation and other areas, join TCG to support TNC. Products for wireless LANs, integrity measurement, and verification, network access, server communication and other functions are announced. Independent demonstrations by the Interop iLabs team include open source Radius server and 802.1x supplicant elements, combined with other products and software.

TCG's Mobile Phone Work Group announces its Mobile Trusted Module (MTM) specification for enabling trust and security in mobile phones. Industry analysts, as well as the mobile standards organizations creating complementary specifications, praise the TCG's efforts to provide non-proprietary solutions to the issues of mobile data, transactions, and content.

2007
In first quarter, TCG announces revised specifications for TNC that add support for Java and VoIP endpoints.

TCG announces a number of new members and hosts its first hands-on workshop at RSA 2007.

In May 2007, at Interop Las Vegas 2007, TCG announces interoperability of the TNC architecture with Microsoft's Network Access Protection (NAP) architecture, enabling products based on TNC specifications to work with Windows clients and servers and vice versa. This interoperability, previously promised by Microsoft and TCG, opens up a number of NAC deployment options for customers, preserves investments and reduces confusion in the NAC market for both customers and vendors.

June 2007, the group announces its Trusted Storage specification that enables full security of local drives on PCs. The group will work to extend this trusted storage to other storage devices. Later this year, the work group announces its first application note for key management and a new subgroup dedicated to trusted optical drive devices.

TCG's mobile work group makes available its Mobile Reference Architecture specification mid-year. This is the first open, hardware-assisted security standard for mobile trusted platforms that

will use the Mobile Trusted Module (MTM) based on a specification published in September 2006.

2008

In January, FreeRADIUS, on open source Radius server implementation, announces a new release that adds support for TNC. It joins a number of other open source implementations and products for TNC.

Also in the first quarter, as part of its ongoing commitment to the IETF and that group's Network Endpoint Assessment (NEA) working group, TCG submits the IF-TNCCS (TNC client-server) 2.0, IF-M (measurement) 1.0 and IF-M Security specifications to the IETF. The IETF NEA working group decides to adopt these specifications as the basis for developing a set of IETF RFCs.

In April 2008, the TNC work group announces a major extension to the TNC architecture. Moving beyond pre-admission control, the architecture now can support post-admission control via its new IF-MAP (Interface Metadata Access Point) protocol.

The new protocol provides a powerful publish/subscribe model that allows data from a variety of networking and security devices and applications to be collected and communicated throughout the network. During this time, new members Arcsight, nSolutions, Lumeta, and others join TCG to work on this effort. Demos are shown at Interop 2008 alongside demos of existing TNC capabilities including the NAP/TNC statement of health and others

The organization announces the Japan Regional Forum in June 2008 to help promote and foster development of products and services based on TCG specifications.

In the fall of 2008, the organization announces a deep set of development tools and resources from member companies to help foster development of applications for the TPM.

2009

TCG's Storage Work Group releases final specifications for self-encrypting drives for laptops and data centers and a set of APIs to enable interoperability among vendors who design the drives.

In April 2009, the organization rolls out its first certification program, targeted to TPMs. The program provides a minimum level of required security and helps ensure interoperability and adherence to the TCG specifications. It is announced that the next certification program will be for products using the Trusted Network Connect network security specifications.

TNC announces a focus on "Pervasive Security" with new support for remote access, clientless endpoints and federated ID; a variety of TNC implementations and capabilities are shown at Interop 2009.

The Japan Regional Forum hosts a permanent demonstration showcase in Tokyo.

TPM is recognized as an international standard by ISO. In other international developments, TCG forms a second regional body, the China Regional Forum, for communication and education of the developer and end-user communities.

2010

In January at Storage Visions, TCG members show the first self-encrypting drives based on TCG specifications.

TCG hosts the "Security Playground" at RSA Conference 2010, giving some 500 attendees hands-on interaction with the TPM, self-encrypting drives, and network security based on the TNC specifications.

In March, the Internet Engineering Task Force (IETF) publishes long-awaited network access control standards based on TCG's TNC specifications. In doing so, all products supporting TNC and Microsoft's Network Access Protocol become compatible with products supporting Cisco's flavor of network access control. This basically ends the NAC standards war.

A certification program for TNC is announced with the first set of certified products from several TCG members. Members show a variety of demonstrations of TNC including those incorporating the Metadata Access Protocol (IF-MAP); demonstrations include integration of physical and IT security and SCADA security.

The U.S. National Security Agency hosts the first Trusted Computing Conference and Expo. Speakers from U.S. government agencies, leading vendors, and enterprises address challenges in cyber security. Applications of Trusted Computing, including the Trusted Platform Module, self-encrypting drives and network security, are discussed for the first time by large enterprise users. Hundreds of attendees also see Trusted Computing demonstrations.

TCG announces the Trusted Multi-Tenant Infrastructure Work Group, which will address the role of trust in cloud security.

TNC continues its evolution, announcing updates to the TNC IF-MAP specification and integration of TNC with the SCAP protocol. As a result of the latter, SCAP-validated scanners can now be used with TNC-certified network security gear to identify and quarantine unhealthy devices.

TCG participates in an event hosted by India's national IT and security organization to continue its worldwide outreach.

Estimates of TPMs embedded in various systems approach one billion. The large enterprise PriceWaterhouseCoopers notes its use of the TPM to protect sensitive data.

2011
TCG starts the year with a series of talks and demos about self-encrypting drives at the Storage Visions Conference, demonstrating the increasing availability and adoption of them for data protection.

TCG's Trusted Multi-tenant Infrastructure effort unveils use cases for Trusted Computing-enabled security for cloud computing.

February sees another standing room-only session for TCG, its members and users of Trusted Computing solutions the RSA Conference. PriceWaterhouseCoopers keynotes the event, joined by users from government, healthcare and nonprofits describing their use of Trusted Computing.

A report from the widely regarded Ponemon Institute finds growing acceptance and knowledge of self-encrypting drives with many organizations reporting potential benefits and plans to use such drives.

TCG attends the National Security Agency Trusted Computing Conference and Exposition, which features presentations on a variety of related topics.

Storage industry analysts at Coughlin Associates find that a dramatic shift to self-encrypting drives, both hard disk drives and solid state drives, will occur by 2017. Coughlin also notes that within the next two years, more than 80 percent of HDDs will be self-encrypting based on TCG specifications.

TCG announces its Trusted Virtualized Platform Architecture to support virtualized systems with trust-based security.

Members elect TCG members Dell and Nokia to TCG's board of directors.

2012
TCG hosts yet another well-attended RSA Conference session, with a focus on the paradox of security. Case studies highlight TCG in action at leading enterprises around the world.

TCG announces a new membership option, Associate, Associate, targeted to enterprise users, service providers, and to integrators and resellers. This year, the organization also adds members including Toyota Motor Corporation and more than a dozen others.

New TCG member Cisco and longtime member Juniper Networks take board seats as TCG Promoter members.

TCG teams with Global Platform Alliance to continue driving mobile platform security solutions.

Research from Aberdeen Group notes that enterprises can incur significant savings by deploying a hardware-based root of trust, such as the TPM.

Three new Architect's Guides, focused on mobile security, comply to connect, and BYOD, are published to help users solve their security problems.

TCG attends both the Information Assurance Exposition and the (ISC)2 Congress to demonstrate authentication, self-encrypting drives and network security.

The group estimates the number of trusted endpoints at more than one billion worldwide.

Contact: Anne Price, PR Works, Inc.
+1-602-840-6495
press@trustedcomputinggroup.org